



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/700,786	11/03/2003	Mariusz H. Jakubowski	MS1-1664US	5484
22801 7590 04/09/2008 LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			EXAMINER DEBNATH, SUMAN	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 04/09/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/700,786

Applicant(s)

JAKUBOWSKI ET AL.

Examiner

Suman Debnath

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 21 September 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-9, 11-16, 32-38, 56-58 and 60-71 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9, 11-16, 32-38, 56-58 and 60-71 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/ are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Claims 1-9, 11-16, 32-38, 56-58 and 60-71 are pending in this application.
2. Claims 1, 32, 56 and 57 are currently amended.
3. Claims 10, 39 and 59 are cancelled.
4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

### *Claim Rejections - 35 USC § 101*

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claim 32 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, as they do not fall under any of the statutory classes of inventions. The language in the claim raises an issue because the claims are directed to nonfunctional descriptive material (i.e. a compilation or mere arrangement of data), and as such, the claim would be directed to non-statutory subject matter.

A data structure is defined as a physical or logical relationship among data elements, designed to support specific data manipulation functions. As claimed, “**a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users**” would not fall under this definition and is therefore non-statutory nonfunctional descriptive material. Arrangements of data without any functional interrelationship is not a process, machine, manufacture or composition

of matter. Nonfunctional' descriptive material may be claimed in combination with other functional descriptive multi-media material on a computer-readable medium to provide the necessary functional and structural interrelationship to satisfy the requirements of 35 U.S.C. § 101.

Regarding claims 33-38, they are rejected because of their dependency on the claim 32, and further would not fall under the above definition of data structure and is therefore non-statutory nonfunctional descriptive material.

***Claim Rejections - 35 USC § 103***

7. Claims 1-9, 11-15, 32-38, 56-58 and 60-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener et al. (Pub. No.: US 2003/0105980 A1), hereinafter "Challener" in view of Bailey (Patent No.: US 7,205,883 B2) and Thomlinson et al. (Patent No.: US 6,272,631 B1), hereinafter "Thomlinson".

8. As to claim 1, Challener discloses a method comprising: creating a data structure including a plurality of user id-user key pairs (FIG. 1, [0019]), each user id-user key pair comprising a user id associated with one of a plurality of users (FIG. 1, [0019], [0021]). Challener doesn't explicitly disclose a user key comprising a master key and a keyed-hash message authentication code encrypted using a password associated with the one of the plurality of users; and delivering the data structure to one or more of the plurality of users.

However, Bailey discloses a user key comprising a master key encrypted using a password associated with the one of the plurality of users (FIG. 4, column 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K.....the SAK is wrapped using key K to produce a K-wrapped secondary authentication key..."); and delivering the data structure to one or more of the plurality of users (column 8, lines 7-25, "The [SAK].sub.K is transmitted to the host site...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to a network.

Neither Challener nor Bailey explicitly discloses a user key comprising a master key and a keyed-hash message authentication code. However, Thomlinson discloses a user key comprising a master key and a keyed-hash message authentication code (FIG. 3, lines 30-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

9. As to claims 32 and 56, these are rejected using the same rationale as for the rejection of claim 1.

10. As to claim 57, it is rejected using the same rationale as for the rejection of claim 1.

11. As to claims 2, 33 and 58, Challenger doesn't explicitly disclose wherein the act of delivering comprises delivering the data structure to each of the plurality of users. However, Bailey discloses wherein the act of delivering comprises delivering the data structure to each of the plurality of users (column 8, lines 7-25, "The [SAK].sub.K is transmitted to the host site...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger as taught by Bailey in order to support multiple users in password-based access to a network.

12. As to claims 3 and 60, Challenger discloses a hash of the password associated with the one of the plurality of users (FIG. 1, [0002]). Challenger doesn't explicitly disclose wherein each master key is encrypted using a hash of the password. However, Bailey discloses wherein each master key is encrypted using a hash of the password (FIG. 4, column 8, lines 7-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger as taught by Bailey in order to improve security in password-based access to a network.

13. As to claims 4, 5, 34, 35, 61 and 62, these are rejected using the same rationale as for the rejection of claim 3.

14. As to claims 6, 36 and 63, Challenger discloses wherein each user key has an integrity verification feature associated therewith ([0019], "The phrase signed with the loaded private key is then compared with the stored signed phrase associated with the remote user..").

15. As to claims 7, 8 and 37, neither Challenger nor Bailey explicitly discloses wherein each master key has an integrity verification feature associated therewith. However, Thomlinson discloses wherein each master key has an integrity verification feature associated therewith (column 10, lines 30-65, "The master authentication key is used in conjunction with the specified MAC to verify that the master key decrypted correctly").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

16. As to claims 9, 38 and 64, Challenger discloses wherein each user key includes a checksum ([0002], [0019]).

17. As to claims 65, neither Challenger nor Bailey explicitly discloses wherein each user key includes a keyed-hash message authentication code. However, Thomlinson discloses a user key comprising a master key and a keyed-hash message authentication code (FIG. 3, lines 30-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

18. As to claims 11 and 66, neither Challener nor Bailey explicitly discloses transforming data using the master key. However, Thomlinson discloses transforming data using the master key (column 10, lines 30-65, "The master key is then used to decrypt an appropriate item key...").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

19. As to claims 12 and 67, neither Challener nor Bailey explicitly disclose storing data transformed using the master key; and controlling access by the plurality of users to the transformed data. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and controlling access by the plurality of users to the transformed data (column 9, lines 50-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.



20. As to claims 13 and 68, Challenger discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]). Neither Challenger nor Bailey explicitly discloses storing data transformed using the master key; and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 50-67 and column 10, lines 1-10); and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

21. As to claims 14 and 69, these are rejected using the same rationale as for the rejection of claim 13.

22. As to claims 15 and 70, Challenger discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]); selecting a user key from the data structure based on the received user id (FIG. 1, [0019], [0021]). Challenger doesn't explicitly disclose storing data transformed using the master key; decrypting the selected user id using the received password to reproduce the master key; and using the master key to access the data.

However, Bailey discloses decrypting the selected user id using the received password to reproduce the master key (FIG. 4, column 8, lines 7-25, "...K-unwrapping of [SAK].sub.K.").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger as taught by Bailey in order to improve security in password-based access to a network.

Neither Challenger nor Bailey explicitly discloses storing data transformed using the master key; and using the master key to access the data.

However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and using the master key to access the data (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

23. Claims 16 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challenger and further in view of Bailey, Thomlinson and Tewfik et al. (Pub. No.: US 2003/0095685 A1), hereinafter "Tewfik".

24. As to claims 16 and 71, Challenger discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]); selecting a user key from

the data structure based on the received user id (FIG. 1, [0019], [0021]). Hashing the received password to produce a hash value (FIG. 1, [0002]). Challenger doesn't explicitly disclose storing data watermarked using the master key; decrypting the selected user id using the received password to reproduce the master key; and using the master key to access the watermarked data.

However, Bailey discloses decrypting the selected user id using the received password to reproduce the master key (FIG. 4, column 8, lines 7-25, "...K-unwrapping of [SAK].sub.K.>").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger as taught by Bailey in order to improve security in password-based access to a network.

Neither Challenger nor Bailey explicitly discloses storing data watermarked using the master key; and using the master key to access the watermarked data.

However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and using the master key to access the data (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challenger and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

Neither Challenger and Bailey nor Thomlinson explicitly discloses watermarked data. However, Tewfik discloses watermarked data ([0015], [0020]). Therefore it would

have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener, Bailey and Thomlinson as taught by Tewfik in order to protect contents from unauthorized duplication.

25. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

#### ***Response to Amendment***

26. Applicant has amended claims 1, 32, 56 and 57, which necessitated new ground of rejections. See rejection above.

#### ***Response to Arguments***

27. Applicant's arguments have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground (s) of rejection is made. See rejection above.

Application/Control Number:  
10/700,786  
Art Unit: 2135

Page 12

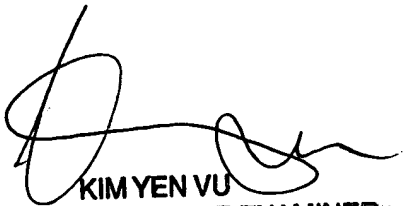
***Conclusion***

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./  
Examiner, Art Unit 2135

  
KIM YEN VU  
SUPERVISORY PATENT EXAMINER